CLAIMS

1. A method for auditing data-access events occurring in a context management system, the method comprising:

(A) collecting context data from a plurality of applications that use the context management system;

(B) storing data corresponding to the collected context data on a centralized storage location; and

(C) extracting audit information by processing at least a subset of the data stored on the centralized storage location.

2. The method of claim 1, wherein the context data comprises user context data items.

3. The method of claim 1, wherein the context data comprises patient context data items.

4. The method of claim 3, further comprising:

(D) appending an application-identifying tag to a URL to yield a compound URL; and

(E) exchanging the compound URL with an application such that future communications with the application allow a context manager to identify the application from the application-identifying tag.

5. The method of claim 1, wherein the audit data comprises application-identifying information.

6. The method of claim 1, wherein the data corresponding to the collected context data is the same as the context data.

7. The method of claim 1, wherein the context management system supports the CCOW standard set.

8. The method of claim 1, wherein any of the plurality of applications supports the CCOW standard set.

9. The method of claim 1, wherein the context data is formatted according to the CCOW standard set.

10. The method of claim 1, further comprising, prior to (B), converting the context data between a first format, complying with the CCOW standard set, and a second data format.

11. The method of claim 1, wherein at least a first application executes on a first machine at the point-of-use and at least a second application executes on a second machine.

12. The method of claim 1, wherein at least a first application executes on a first machine comprising a remote server and at least a second application executes on a second machine.

13. The method of claim 1, wherein at least two applications execute on a same machine.

14. The method of claim 1, wherein a first application and a second application are each separate instances of the same application executing simultaneously.

15. The method of claim 1, wherein a first application and a second application are two different applications executing simultaneously.

16. The method of claim 1, wherein the processing in (C) comprises querying the data stored in the centralized storage location.

17. The method of claim 1, wherein the method is performed by software executing on a machine coupled to the centralized storage location over a network.

18. The method of claim 1, wherein the method is performed by software executing on a machine housing the centralized storage location.

19. The method of claim 1, wherein (B) comprises:

(i) storing the context data onto an intermediate collection platform, disposed between the context management system and the centralized storage location; and

(ii) sending the context data from the intermediate collection platform to the centralized storage location.

20. The method of claim 19, wherein the intermediate collection platform comprises a message queue.

21. The method of claim 19, wherein the intermediate collection platform comprises a storage buffer.

22. The method of claim 1, further comprising, following (C):

(D) based on the extracted audit information, determining whether a data access event is authorized under a set of access control rules.

23. The method of claim 22, further comprising, following (D):

(E) preventing execution of the data access event if the data access event is not authorized.

24. The method of claim 22, further comprising, following (D):

(E) sending a message to a monitor, indicating an attempt to execute the data access event.

25. The method of claim 24, wherein the monitor is at least one of: an electronic mail server, a telephony server, a paging server, a portable communicator, an alarm device and a human operator.

26. The method of claim 22, wherein the set of access control rules is accessible to the context management system.

27. The method of claim 1, wherein the method is performed by software, execution of which is not subject to preemption by a user.

28. The method of claim 1, wherein the centralized centralized storage location is a database.

29. The method of claim 1, further comprising:

(D) passing the context data between a first application and a second application using a context manager.

30. The method of claim 1, further comprising:

(D) collecting active-application data indicative of which of the plurality of applications is in immediate use by a user.

31. The method of claim 1, further comprising, prior to (C):

(D) granting an authorized auditor access to the centralized storage location.

32. The method of claim 1, further comprising, prior to (C):

(D) collecting point-of-use data identifying a point-of-use machine.

33. The method of claim 1, further comprising:

(D) evaluating the audit data to make an assessment of compliance with a set of regulations.

34. The method of claim 33, wherein the set of regulations corresponds to the HIPAA.

35. The method of claim 1, wherein (B) comprises storing of the context data according to a synchronization scheme that combines into the centralized storage location context data from at least two sources.

36. A method for storing context data, from a plurality of sources in a context management system, onto a centralized storage location, comprising:

(A) receiving context data from the plurality of sources;

(B) synchronizing the context data using a context manager; and

(C) storing the context data in the centralized storage location;

wherein (C) is performed according to a synchronization scheme, that includes context data from at least two sources.

37. The method of claim 36, wherein the centralized storage location is accessed over a network.

38. The method of claim 36, further comprising, prior to (C):

(D) storing the context data on a plurality of intermediate clustered storage locations sharing a centralized index.

39. The method of claim 36, wherein the synchronization scheme is chronological.

40. The method of claim 36, wherein the synchronization scheme is not application-vendor-specific.

41. The method of claim 36, further comprising:

(D) converting the context data from a first data format to a second data format.

42. A method for controlling access to a stored data object, comprising: determining whether a data-access event is authorized under a predetermined rule, wherein a context manager is operable to allow or deny execution of said data-access

event based on (i) context data, corresponding to the data-access event, and (ii) the predetermined rule.

43. The method of claim 42, further comprising determining whether the data-access event is authorized based on determining whether a context gesture corresponding to the data-access event is authorized.

44. The method of claim 42, wherein the context manager is operable to allow or deny execution of the data-access event.

45. The method of claim 42, further comprising: storing a record of the data-access event on a centralized storage location coupled to the context manager.

46. A method for assessing compliance with the HIPAA, in a context management system, the method comprising:

(A) collecting context data from a plurality of applications that use the context management system;

(B) storing data corresponding to the collected context data on a centralized storage location; and

(C) extracting audit information by processing at least a subset of the data stored on the centralized storage location, the audit information suitable for making an assessment of compliance with a provision of the HIPAA.

47. The method of claim 46, wherein any of the plurality of applications supports the CCOW standard set.

48. The method of claim 46, wherein the plurality of applications exchange context data through a context manager operating in a healthcare facility and the context data relates to patient records.

49. A method for auditing data access events in a data processing system, comprising:

(A) transferring context information from a first software application executing in the data processing system to a second software application executing in the data processing system;

(B) storing the context data in a centralized storage location; and

(C) extracting from the centralized storage location information indicative of data access events occurring in the data processing system.

50. A data processing system for auditing data access events in a context management framework, comprising:

a plurality of software applications executing in the data processing system;

a context manager coupled to the software applications that manages context data exchanges between the software applications;

a centralized storage location, coupled to the context manager, that stores a central record of the context data exchanges; and

an auditor, coupled to the centralized storage location, that retrieves information from the centralized storage location indicative of data access events occurring in the data processing system.

51. The system of claim 50, further comprising a network that connects the context manager to the centralized storage location.

52. The system of claim 50, further comprising a machine that hosts both the context manager and the centralized storage location.

53. The system of claim 50, further comprising a first machine that executes a first software application and a second machine that executes a second software application.

54. The system of claim 53, wherein the first machine is a local point-of-access machine and the second machine is coupled to the first machine over a network.

55. The system of claim 53, wherein the first machine is a remote server and the second machine is coupled to the first machine over a network.

56. The system of claim 50, wherein the software applications comply with the CCOW standard set.

57. The system of claim 50, further comprising a data formatter, arranged to convert data passing between the context manager and the centralized storage location between a first format, supported by the CCOW standard set, and a second format.

58. The system of claim 50, further comprising communication signals carrying context data.

59. The system of claim 50, further comprising a message dispatcher that sends a message to a monitor based on an output from the auditor.

60. The system of claim 59, wherein the monitor comprises at least one of: an electronic mail server, a telephony server, a paging server, a portable communicator, an alarm device and a human operator.

61. The system of claim 50, further comprising an authorizer that determines whether a data access event is authorized.

62. The system of claim 61, further comprising an access controller that controls data-access events responsive to an output from the authorizer.

63. The system of claim 50, wherein the centralized storage location comprises a database.

64. The system of claim 50, further comprising a plurality of clustered storage locations sharing a common index, the clustered storage locations holding data used by the context manager.

65. The system of claim 50, further comprising an intermediate collection platform disposed between the context manager and the centralized storage location.

66. The system of claim 65, wherein the intermediate collection platform comprises a message queue.

67. The system of claim 65, wherein the intermediate collection platform comprises a storage buffer.

68. The system of claim 50, further comprising means for blocking execution of a data-access event on a machine coupled to the system.

69. The system of claim 50, further comprising a Web-proxy that converts communications between a first, World Wide Web-based, format and a second format.

70. The system of claim 69, wherein the second format is COM-based.

71. The system of claim 69, further comprising a Web interface coupled between the context manager and the Web-proxy.

72. A machine-readable medium having thereon instructions, which when executed:

(A) collect context data from a plurality of applications that use a context management system;

(B) store data corresponding to the collected context data on a centralized storage location; and

(C) extract audit information by processing at least a subset of the data stored on the centralized storage location.

73. The medium of claim 72, wherein any of the plurality of applications supports the CCOW standard set.

74. The medium of claim 72, further having instructions, which when executed:

(D) convert context data from a first data format to a second data format.

75. The medium of claim 74, wherein any of the first and second data formats is according to the CCOW standard set.

76. The medium of claim 72, wherein the centralized storage location comprises a database.

77. The medium of claim 72, wherein (B) comprises sending data over a network coupling the context manager and the centralized storage location.

78. The medium of claim 72, further having instructions, which when executed:

(D) couple application-identification information to a URL being delivered through the context manager.

79. The medium of claim 72, further having instructions, which when executed:

(D) determine whether a data-access event is authorized under a set of access control rules.

80. The medium of claim 79, further having instructions, which when executed:

(E) prevent execution of the data-access event if the data-access event is not authorized.

81. The medium of claim 79, further having instructions, which when executed:

(E) send a message to a monitor, indicating an attempt to execute the data-access event.

82. The medium of claim 81, wherein the monitor is at least one of: an electronic mail server, a telephony server, a paging server, a portable communicator, an alarm device and a human operator.

83. The medium of claim 79, wherein (D) comprises comparing context data to a rule available to the context manager.

84. The medium of claim 72, wherein execution of the instructions is performed by software, execution of which is not subject to preemption by a user.

85. A method for identifying an application in a context management environment, wherein the application is coupled to a context manager, comprising:

(A) associating the application with an information tag when the application invokes a method that carries application-identifying information;

(B) augmenting a URL, passing between the context manager and the application, with the information tag, yielding a compound URL containing the URL and the information tag;

(C) parsing a communication from the application containing the compound URL to extract information corresponding to the information tag therefrom when the application invokes a method that does not carry application-identifying information; and

(D) looking up the identity of the application corresponding to the information tag.

86. The method of claim 85, further comprising: converting communications between a first Web-based format and a second format.